

**BY ORDER OF THE  
SECRETARY OF THE AIR FORCE**



**AIR FORCE INSTRUCTION 14-119**

**15 AUGUST 2007**

**AIR EDUCATION AND TRAINING  
COMMAND  
Supplement**

**30 JANUARY 2009**

***Intelligence***

**INTELLIGENCE SUPPORT TO FORCE  
PROTECTION (FP)**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** This AFI is available for downloading from the e-Publishing website at <http://www.e-publishing.af.mil>.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: HQ USAF/A2AF  
Supersedes: AFI14-119, 6 January 2004

Certified by: HQ USAF/A2A  
(Mr. Steven A. Cantrell)

Pages: 38

**(AETC)**

OPR: HQ AETC/A2OI  
Supersedes: AFI14-119\_AETCSUP1,  
7 March 2005

Certified by: HQ AETC/A2/30  
(Lt Col Tal Metzgar)

Pages: 13

---

This instruction provides guidance to support force protection mission execution, encompassing peacetime through wartime operations. It implements Air Force Policy Directive (AFPD) 10-2, *Readiness*, AFPD 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources and Operations*, AFPD 14-3, *Control, Protection and Dissemination of Intelligence Information*, AFPD 31-3, *Air Base Defense*, Air Force Doctrine Document (AFDD) 2-4.1, *Force Protection*. Use in conjunction with Air Force Instruction (AFI) 14-104, *Oversight of Intelligence Activities* and AFI 14-105, *Unit Intelligence Mission and Responsibilities*, and with other higher headquarters (HHQ) directives and local guidance. This AFI applies to Air Force Reserve Command (AFRC) and Air National Guard (ANG) units. This instruction does not address all missions or responsibilities of Air Force Intelligence units that perform specialized force protection functions (i.e., Contingency Response Groups [CRG]). This instruction provides HHQ guidance for the development of Air Force Major Command (MAJCOM) Instructions. HQ USAF/A2 must approve any deviations from or revisions to this instruction. Approval for deviations will be in the form of a command supplement or waiver. Waivers will be considered if compliance will adversely affect mission accomplishment, exceed local

capabilities or require substantial expenditure of funds at a location where forces will be removed or relocated in the near future. Send all recommended changes for this publication to HQ USAF/A2AF. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123 (will convert to AFMAN 33-363), *Management of Records*, and disposed of in accordance with Air Force Records Disposition Schedule (RDS) located at <https://afrims.amc.af.mil>.

This publication may require the collection and or maintenance of information protected by the Privacy Act (PA) of 1974. The authorities to collect and or maintain records prescribed in this publication are Title 37 *United States Code*, Section 301a and Executive Order 9397, *NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL PERSONS*, November 22, 1943.

**(AETC) This supplement implements and extends the guidance of AFI 14-119, *Intelligence Support to Force Protection (FP)*, 15 August 2007.** It applies to all AETC units and members; and to AETC-gained Air National Guard and Air Force Reserve Command (AFRC) units and members. Forward requests for waivers to this supplement to HQ AETC/A2OI, identify the specific requirements to be waived and include justification. If approved, a waiver stays in effect for the life of the publication unless HQ AETC/A2OI specifies a shorter period of time, cancels it in writing, or issues a change to the waiver. Ensure that all records created as a result of processes prescribed in this publication are maintained according to AFMAN 33-363, *Management of Records*, and disposed of according to Air Force Records Disposition Schedule located at <https://www.my.af.mil/gcss-af61/afrims/afrims>. Send suggested improvements to this supplement on AF Form 847, *Recommendation for Change of Publication*, through command channels to HQ AETC/A2OI, 1 F Street, Suite 2, Randolph AFB TX 78510-4325.

## ***SUMMARY OF CHANGES***

This document has been substantially revised and must be completely reviewed. Major changes include: reorganization of information, incorporating Iraq and Afghanistan Lessons Learned and clarifying intelligence responsibilities, specifically for host, tenant and expeditionary units, as well as Air Force Office of Special Investigation (AFOSI)/Intelligence FP roles.

## **MISSION AND RESPONSIBILITIES**

**(AETC) This document has been substantially revised and must be completely reviewed.** It clarifies intelligence responsibilities at the unit level and provides guidance on documenting the critical infrastructure program (CIP) (paragraph 4.1.7); introduces processes and procedures in an operating instruction (paragraph 4.1.2); updates document processes and procedures in compliance with higher headquarters (HHQ) standards (paragraph 4.1.22.1); establishes intelligence training and responsibilities for AETC units without intelligence personnel assigned (5.1.9); and provides and establishes responsibilities for tenant unit intelligence responsibilities (7.1).

1.	Mission. ....	3
2.	AFOSI Responsibilities .....	4

3.	HQ USAF/A2 R .....	5
4.	MAJCOM Intelligence Responsibilities: .....	5
5.	Host Unit (In-garrison) Intelligence Responsibilities: .....	9
6.	Expeditionary Intelligence Responsibilities: .....	14
7.	Tenant Unit Intelligence Responsibilities .....	17
8.	(Added-AETC) Form Adopted. ....	18
<b>Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>		<b>19</b>
<b>Attachment 2—(Added-AETC) CIP INTELLIGENCE REQUIREMENTS</b>		<b>28</b>
<b>Attachment 3—(Added-AETC) INTELLIGENCE SUPPORT CHECKLISTS</b>		<b>36</b>

**1. Mission.** The 1996 attack on the Khobar Towers apartment building at Dhahran Air Base, Saudi Arabia that killed nineteen Airmen and wounded hundreds of US service members transformed the way the Air Force views FP. All Airmen are subject to threats whether in the Continental United States (CONUS), Outside the Continental United States (OCONUS) or deployed to expeditionary bases. Asymmetric threats will increasingly challenge US personnel, facilities and assets. Understanding how these threat elements conduct attacks is the first step to developing an effective Antiterrorism (AT) program that will help commanders assess their ability to prevent, survive, and prepare to respond to an attack. Providing threat information to support the planning and execution of FP operations requires changing our culture and the way commanders use and deploy intelligence personnel, products and services. Intelligence personnel must be organized, trained and equipped to support FP customers and help protect personnel, resources and information from threats that could destroy, damage or compromise the capability of the Air Force to perform its assigned missions. FP customers include, but are not limited to: commanders, aircrews, Security Forces (SF), Explosive Ordnance Disposal (EOD), Civil Engineers (CE), Medical, Antiterrorism Officers (ATO), PHOENIX RAVENS, AFOSI, Threat Working Groups (TWG), FP Working Groups (FPWG) and Base Defense Operations Centers (BDOC).

1.1. AFI 14-105 directs the development, implementation and execution of an FP support program as an integral part of the Wing/Base Installation Commander's FP Program. Intelligence personnel at all levels will work in coordination with their cross-functional counterparts (e.g., AFOSI, SF, ATOs, etc.) to ensure FP threat/intelligence requirements are satisfied.

1.2. Force Protection Intelligence (FPI) is analyzed, all-source information concerning threats to Department of Defense (DOD) missions, people or resources arising from terrorists, criminal entities, Foreign Intelligence and Security Services (FISS) and opposing military forces. FPI supports FP decisions and operations and is performed collaboratively by Intelligence, AFOSI, and Security Forces personnel. Intelligence supports unit deployments, readiness training, mission planning and other mission execution functions. Intelligence provides the following support to all phases of FP operations:

1.2.1. Indications and Warning (emerging crisis situations).

1.2.2. Current Intelligence (adversary intentions, courses of action).

1.2.3. General Military Intelligence (adversary Order of Battle (OB), cultural awareness information).

1.2.4. Near-Real-Time/Real-Time Situational Awareness.

1.2.5. Intelligence Preparation of the Battlespace (IPB) (terrain analysis, route analysis, Man-Portable Air Defense System [MANPADS]/stand-off weapons footprints, adversary capabilities, tactics, techniques and procedures [TTPs], etc.).

1.2.6. Target Intelligence (target study, target folder development).

1.2.7. Combat Assessment (pre-/post-mission briefings/debriefings, mission assessment).

1.2.8. Scientific and Technical Intelligence (weapon characteristics, capabilities, vulnerabilities, limitations and effectiveness).

1.3. In Accordance With (IAW) AFI 14-105, intelligence personnel will not be assigned additional duties that interfere with their contingency/wartime taskings or intelligence responsibilities. Intelligence personnel will not be designated as augmentees for other base functions during wartime, contingencies or exercises.

1.4. IAW AFI 14-104, units have specific operational parameters regarding what and how they can collect, retain and disseminate information with respect to US persons. This AFI should not be interpreted as authorization for intelligence personnel to collect and maintain information on US persons; the unit must have an authorized mission to do so. Information about a US person may be collected by AFOSI in its role as a designated counterintelligence (CI) component if it is necessary to perform its assigned mission.

1.5. Intelligence personnel supporting FP should coordinate with an appropriate legal advisor on topics and products concerning FP legal considerations, Law of Armed Conflict (LOAC), or Intelligence Oversight (IO).

## **2. AFOSI Responsibilities**

2.1. AFOSI is the lead Air Force agency for collection, investigation, analysis and response for threats arising from terrorists, criminal activity and foreign intelligence and security services (FISS). AFOSI is primarily focused on countering adversary intelligence collection activities against US forces. FP customers must request information, products and services on these types of threats from their servicing AFOSI Field Investigative Region (FIR)/Detachment (Det). AFOSI responsibilities include:

2.1.1. Provide information and products on terrorist threats.

2.1.2. Neutralize enemy and terrorist threats with appropriate US and allied forces.

2.1.3. Within its investigative jurisdiction, identify and investigate crimes against people, private and government property; fraud; technology transfer violations; terrorism; etc.

2.1.4. Act as Air Force single point of contact for conducting CI collections, investigations and offensive CI operations; collect, analyze, and disseminate CI threat information.

2.1.5. Act as Air Force lead for locating and tracking enemy and terrorist operatives threatening US/allied personnel and resources through investigative operations outside of established foreign base perimeters and IAW applicable international agreement.

2.1.6. Investigate intrusion/intentional sabotage of DOD computer systems.

2.1.7. Act as Air Force single point of contact with federal, state, local and foreign nation Law Enforcement (LE), CI and security agencies.

2.1.8. Develop a Defense Threat Assessment (DTA) for all Air Force installations that identifies the full range of terrorist capabilities that could reasonably be used against the installation or its personnel, including all likely Weapons of Mass Destruction (WMD)/Counter Biological, Radiological, Nuclear, Explosive (CBRNE) threats.

2.1.9. Serve as the installation-level training agency for CI Awareness briefings (e.g., AT Level I training) that include: all pertinent terrorist threats, threats to the specific installation or mission and specific security vulnerabilities of the installation.

2.1.10. Provide CI threat assessments to deploying Air Force units.

2.1.11. Operate 24-hour operations center to receive and disseminate worldwide terrorist threat information.

### 3. HQ USAF/A2 R esponsibilities

3.1. Provide policy for planning, programming, training and budgeting resources necessary to ensure the Air Force has the capability to collect, analyze, produce and disseminate all-source intelligence information to support FP operations, excluding all policy pertaining to CI (with the exception of policy regarding Intelligence Oversight).

3.2. Coordinate on Air Force, DOD and Intelligence Community (IC) policies affecting intelligence support to FP.

3.3. Produce substantive intelligence for Secretary of the Air Force (SecAF), Chief of Staff (CSAF), operations planners and their staff. Review all-source intelligence effecting Air Force security/FP posture and recommend courses of action to the Headquarters Air Force (HAF) TWG and senior Air Force leaders. Support 24-hour/7 day-a-week crisis and contingency operations. Represent the Air Force in Director of National Intelligence (DNI), DOD and IC venues.

3.4. Maintain Force Protection website located at: <http://www.afiaa.hq.af.smil.mil> (Secret-level) or <http://www.afiaa.ic.gov> (Top-Secret level).

**4. MAJCOM Intelligence Responsibilities:** Coordinate terrorism-related products (i.e. daily intelligence summaries, terrorist handbooks, threat documents and briefings, etc.) and services with AFOSI to de-conflict work responsibilities and ensure customer requirements are satisfied.

4.1. **Planning and Direction** : Organize, train, and equip forces. Establish guidance for, program for, allocate resources for and manage all command FP-related intelligence requirements. MAJCOMs should tailor the responsibilities listed in this section based upon FP customer requirements, location and mission/area of operation. Send copies of MAJCOM supplements to this AFI to HQ USAF/A2AF.

- 4.1.1. Develop and implement an intelligence FP program in coordination with the servicing Combatant Command (COCOM) and AFOSI Region; report shortfalls/new requirements to AF/A2AF.
- 4.1.2. Coordinate on MAJCOM and HHQ policies affecting intelligence support to FP and coordinate FP policies with installations, as appropriate.
- 4.1.2. (AETC) Document processes and procedures in compliance with higher headquarters (HHQ) standards and guidance in an operating instruction.
- 4.1.3. When applicable, determine responsibilities and roles of intermediate headquarters' intelligence organizations (e.g., Warfighting Headquarters [WFHQ], Numbered Air Force, [NAF]).
- 4.1.4. Develop a minimum list of FP intelligence documents and products, as well as appropriate formats (i.e. hard copy, CD-ROM, web links, etc.) for subordinate and supported units and provide for these requirements.
- 4.1.5. Coordinate intelligence exercise activities and requirements.
- 4.1.6. In coordination with AFOSI, analyze all-source intelligence and provide warning to subordinate units and commanders. Establish procedures to rapidly receive, evaluate, analyze and disseminate all relevant intelligence threat data to AFOSI, subordinate and in-transit units, and FP customers. Ensure procedures are established to track IC terrorism threat levels, terrorism warnings, alerts and advisories.
- 4.1.7. Participate in the MAJCOM TWG and FPWG.
- 4.1.7. (AETC) The AETC senior intelligence officer (SIO) will designate, in writing, an intelligence professional or civilian equivalent to the AETC Threat Working Group (TWG) and AETC force protection working group (FPWG). Intelligence personnel at all levels will work in coordination with their cross-functional counterparts (such as Air Force Office of Special Investigations (AFOSI), security forces, anti-terrorism officer (ATO), critical infrastructure program (CIP), etc.) to ensure FP threat and/or intelligence requirements are satisfied.
- 4.1.8. Ensure procedures, systems and/or databases are in place to incorporate real world and exercise lessons learned, trends and best practices into FP policies and procedures.
- 4.1.9. Conduct intelligence staff assistance visits (SAV) to subordinate units as a medium for intelligence FP process improvement; evaluate readiness; assist in training.
- 4.1.10. Analyze, advocate and staff subordinate units' intelligence resource issues (e.g., manpower, security clearances, systems, facilities and information/production requirements). Coordinate personnel Sensitive Compartmented Information (SCI) access and SCI facility requirements with the supporting Special Security Office (SSO).
- 4.1.11. Ensure subordinate units satisfy FP customer requirements. For subordinate installations without an organic intelligence capability, ensure threat information is available to installation FP customers.
- 4.1.11. (AETC) The base ATO at AETC installations that do not have intelligence professionals permanently assigned will establish procedures to ensure threat information

is available to the installation commander (such as assigning nonintelligence personnel to fulfill FP responsibilities listed in this publication).

4.1.12. Assess subordinate installations' ability to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack and assist AFOSI in fusing suspicious activity reports from security forces, law enforcement, and CI organizations with national-level Intelligence Surveillance and Reconnaissance (ISR) collection activities. Identify and document intelligence-related findings, observations and best practices and update FP programs/policies as needed.

4.1.13. Review Vulnerability Assessment (VA), Operational Readiness Inspection (ORI), Unit Compliance Inspection (UCI), Nuclear Surety Inspection (NSI), etc., intelligence-related observations, findings, and best practices; update FP programs/policies as needed.

4.1.14. In coordination with AFOSI, review subordinate units' DTAs (see paragraph 2.1.8).

4.1.15. Advocate fielding of automated intelligence systems and related training, connectivity and maintenance of systems. Establish and coordinate system requirements with subordinate and gained organizations.

4.1.16. Ensure mission planning materials are available IAW AFI 14-105.

4.1.17. Establish compliance criteria that give clear guidance on unit programs and their expected results.

4.1.18. Provide oversight of intelligence FP unit type code (UTC) management and inform the Air Staff Functional Manager of any FP UTC-related problems, as applicable. Provide assistance in addressing contingency or exercise-related manpower, equipment and communication requirements. Provide list of minimum requirements for mobility equipment.

4.1.19. IAW AFI 31-301, *Air Base Defense*, coordinate with the servicing COCOM and AFOSI FIR/Det. to develop a command threat assessment.

4.1.20. IAW AFI 32-3001, *Explosive Ordnance Disposal Program*, MAJCOMs that have responsibility for EOD will provide threat support and products for EOD programs.

4.1.21. Obtain customer feedback on intelligence products and services.

4.1.22. Oversee, inspect, exercise, assess, and report to HQ USAF/A2 (via AF/A2AF) NLT 30 January of each year on intelligence FP programs for the previous calendar year. This report will help identify intelligence FP issues to influence policy and decision-making efforts. Reports will address the following: 1) summary of MAJCOM's FP program/strategy; 2) trend items (e.g., items that either occur in multiple units or have a significant negative impact on the conduct of FP); 3) best practices (e.g. products, processes); 4) issues for HHQ advisement that are beyond the scope of the MAJCOM's ability to correct or implement and 5) actions/recommendations taken to address issues.

4.1.22. (AETC) Units will report any inspections, exercises, or assessments to HQ AETC/A2OI no later than 30 December of each year on intelligence FP programs for the previous calendar year. Reports will address program summary; negative discrepancies

(noted from staff assistance visits, operational readiness inspections (ORI), and/or vulnerability assessments); best practices; and issues regarding actions or recommendation for HHQ. **Note:** *Does not apply to AFRC. Operational control (OPCON) of AFRC units does not reside in AETC for nonmobilized units. AFRC units report through AFRC.*

#### 4.2. Collection and Requirements Management

4.2.1. Develop MAJCOM FP-related Priority Intelligence Requirements (PIRs) in cooperation with FP customers to drive both theater and national ISR and CI collections.

4.2.2. Establish FP Production Requirement (PR) and dissemination management policy and validate unit and force level FP intelligence requirements IAW HHQ guidance.

4.2.2. (AETC) Identify and submit intelligence production requirements (PR) according to AFI 14-105/AETC Sup 1, *Unit Intelligence Mission and Responsibilities*.

4.2.3. Coordinate with theater and national intelligence organizations, to include AFOSI, and submit collection requirements (CRs) and PRs to satisfy MAJCOM FP PIRs.

4.2.4. In coordination with FP customers, continually assess how well FP PIRs are being satisfied to help guide intelligence and CI collection efforts. Monitor and evaluate reporting against FP requirements.

4.2.5. Champion enhanced production requirements of SECRET collateral-level tearline reporting to ensure the widest possible dissemination of FP threat information.

#### 4.3. Training Support

4.3.1. Provide written guidance on requirements for unit external and internal intelligence FP training, Initial Qualification Training (IQT), Mission Qualification Training (MQT) and Continuation Training (CT). Intelligence personnel should receive certification as external and internal intelligence trainers IAW paragraph 5.3.2.1 and 5.3.3.3. Ensure they are certified in areas on which they provide instruction prior to conducting training.

4.3.1.1. (Added-AETC) Intelligence support to FP training guides and guidelines can be located at the Secret level <http://www.afiaa.hq.af.smil.mil> or Top Secret level at <http://www.afiaa.ic.gov>. All personnel will be trained on intelligence support to FP on an annual cycle.

4.3.1.2. (Added-AETC) Coordinate with appropriate point of contact for internal and external training requirements and establish a lesson plan tailored to unit and base mission, in addition to wartime and deployed taskings. Documentation of completed training will be placed in continuity book.

4.3.2. Provide Subject Matter Expert (SME) support to Utilization and Training workshops to ensure intelligence technical school and advanced skills training curricula prepare intelligence professionals to fulfill FP responsibilities.

4.3.3. In coordination with FP customers, integrate the use of and/or update intelligence into FP customers' training courses, as applicable (e.g. Security Forces Regional Training Centers [RTCs], AT Level II Courses, etc.). Support the command's annual review of their AT Level II Course Curriculum.

4.3.4. Update individual training records to reflect FP training IAW AFI 36-2201.

4.3.5. Annually solicit intelligence units' formal FP training requirements for the subsequent year and coordinate requirements with appropriate agencies.

4.3.6. Annually provide a MAJCOM-sponsored list of recommended FP training opportunities to increase subordinate units' awareness of available training courses.

**5. Host Unit (In-garrison) Intelligence Responsibilities:** Host units are defined as wing/base/center/Operations Support Squadron/Flight (OSS/OSF) with base operating support (BOS)/FP responsibilities for their CONUS/OCONUS in-garrison location. Coordinate terrorism-related products (i.e. daily intelligence summaries, terrorist handbooks, threat documents and briefings, etc.) and services with AFOSI to de-conflict responsibilities and ensure customer requirements are satisfied.

#### 5.1. Planning and Direction

5.1.1. Develop, implement and execute an FP support program as an integral part of the Installation Commander's FP Program. The program will identify which elements, both at home and/or deployed, require intelligence support to perform their FP functions and tailor intelligence products to meet customer needs.

5.1.1.1. Designate in writing primary and alternate intelligence personnel (officer, non-commissioned officer (NCO), civilian and/or contractor) to provide intelligence support for FP. Individuals should have appropriate clearances and access to Top Secret (TS), SCI, Human Intelligence (HUMINT) Control System (HCS) and Gamma (G) data. Individuals requiring these clearances will work through their unit and MAJCOM Director of Personnel to change their Unit Manning Document (UMD) position(s) to reflect the need for an SCI clearance.

5.1.1.2. Ensure personnel performing FP duties receive appropriate training.

5.1.2. IAW MAJCOM guidance and coordination with AFOSI, ensure threat information, products and services are provided to subordinate units, to include Geographically Separated Units (GSUs) (e.g., Munitions Support Squadrons) that do not have an organic intelligence capability, based upon FP customer intelligence requirements.

5.1.3. Plan, program, budget, validate, and manage all intelligence FP requirements for the installation and subordinate units.

5.1.4. Oversee training for intelligence FP personnel, including assigned/attached Individual Mobilization Augmentees (IMAs).

5.1.5. Allocate, assign and manage all intelligence FP personnel resources, to include exercise and/or contingency tasking.

5.1.6. Coordinate on all policies affecting intelligence support to FP.

5.1.7. Ensure intelligence FP Geospatial Information and Services (GI&S) requirements are identified IAW HHQ and MAJCOM guidance derived from AFI 14-205, *Geospatial Information and Services (GI&S)* and sufficient stocks are maintained for training and readiness, deployment and employment. Units must refer to theater guidance for additional GI&S requirements prior to deployment.

5.1.8. Adhere to requirements and policies contained in AFI 16-201, *Air Force Foreign Disclosure and Technical Transfer Program*, for disclosing classified and controlled unclassified (i.e. For Official Use Only [FOUO], tech orders, schematics, etc.). FP military information to foreign nationals. All classified and controlled unclassified FP military information must be reviewed and approved by a properly designated disclosure authority before release. Contact MAJCOM Foreign Disclosure Office for guidance.

5.1.9. Conduct periodic reviews (at least annually) of written FP guidance to ensure currency, accuracy, appropriateness and applicability.

5.1.9. (AETC) Conduct internal and external training at a minimum semiannually or as needed for FP issues relevant to unit operations.

5.1.10. Develop and implement a FP intelligence unit self-assessment program.

5.1.11. Review all plans (e.g., installation AT Plan) at least annually and write intelligence annexes to identify all required intelligence support and information requirements.

5.1.12. Ensure unit personnel and assigned IMAs are fully qualified to fill mobility slots, to include SCI eligibility requirements. Coordinate SCI requirements with the SSO.

5.1.13. Establish and document procedures for providing intelligence products and services to FP customers.

5.1.14. Participate in the TWG and other venues (e.g. FPWG, BDOC) as appropriate.

5.1.15. Analyze all-source intelligence for impact on unit mission and rapidly disseminate threat to FP customers, subordinate and lateral units, HHQs and other appropriate agencies, in coordination with AFOSI.

5.1.15. (AETC) Provide FP Intelligence support and terrorist threat advisories to base organizations such as the threat working group (TWG), FPWG, battle staff, air base operations and/or defense and tenant organizations as needed.

5.1.16. Provide support to FP customers through current, relevant intelligence products and briefings, focusing on enemy activities, capabilities, tactics, weapons, intentions and probable courses of action (COAs).

5.1.16. (AETC) Ensure FP is addressed in current intelligence briefings, pre-mission and pre-deployment briefings.

5.1.17. Establish procedures to track IC terrorism threat levels, terrorism warnings, alerts and advisories in coordination with AFOSI.

5.1.17. (AETC) In coordination with the TWG, fuse all-source intelligence with counter intelligence and law enforcement information provided by AFOSI to analyze terrorist group patterns of behavior and identify evolving threats.

5.1.18. Ensure continuity books are maintained. Continuity books should include:

5.1.18.1. Appointment memo.

- 5.1.18.1. (AETC) Forward copy of appointment memorandum to HQ AETC/A2OI. **Note:** Does not apply to AFRC, OPCON of AFRC units does not reside in AETC for nonmobilized units. AFRC units report through AFRC.
- 5.1.18.2. AFI 14-105, AFI 14-119, AFI 10-245 and MAJCOM supplements.
- 5.1.18.3. Air Force Pamphlet (AFPAM) 14-118, *Aerospace Intelligence Preparation of the Battlespace*, AF Tactics, Techniques, and Procedures (AFTTP) 3-10.1, *Integrated Base Defense*.
- 5.1.18.4. Local Operating Instructions (if applicable).
- 5.1.18.5. Vulnerability Assessment benchmarks.
- 5.1.18.6. Local TWG charter.
- 5.1.18.7. Nuclear Security Threat Capabilities Assessment (as appropriate) and Worldwide Asymmetric Threat to Air Force Installations, Personnel and Resources.
- 5.1.18.8. FP customer requirements.
- 5.1.18.9. Self-inspection/SAV/UCI/ORI/NSI checklists.
- 5.1.18.10. Intelligence portion of the installation AT plan.
- 5.1.18.11. Installation and command threat assessments (e.g. DTA).
- 5.1.18.12. FP PIR List.
- 5.1.18.13. FP Point of Contact List.
- 5.1.18.14. Intelligence Oversight Policy (e.g. AFI 14-104).
- 5.1.18.15. Law of Armed Conflict (LOAC) guidance.
- 5.1.18.16. (Added-AETC) Base imagery and maps highlighting key critical assets, vulnerable terrain areas, and enemy operating area. Include infrastructure within effective range of host units that could be used by adversary to cause a mass casualty event or disrupt critical infrastructure capabilities due to an evacuation.
- 5.1.18.17. (Added-AETC) Terrorist organizations that are active in the AOR and may pose a threat to the installation and personnel.
- 5.1.18.18. (Added-AETC) Copy of working minutes.
- 5.1.18.19. (Added-AETC) Current lesson plan.
- 5.1.18.20. (Added-AETC) Documentation of completed training.
- 5.1.19. Document FP lessons learned and update FP programs appropriately.
- 5.1.19. (AETC) Document intelligence support to FP lessons learned at <https://www.jllis.mil/USAF/> and forward a soft copy to HQ AETC/A2OI for action (as required). Maintain lessons learned for future reference. (See Attachment 3 (Added) for checklists of intelligence support to FP (Table A3.1 (Added) through Table A3.5 (Added).))
- 5.1.20. In coordination with AFOSI, the Inspector General and/or the TWG, develop intelligence scenarios for installation exercises. Ensure scenarios facilitate a practical

simulation of operational intelligence functions and include realistic mission area threats including those posed by transnational terrorists and other opposing military forces.

5.1.21. Support/participate in ORIs, UCIs, SAVs, VAs, NSIs, MIGHTY GUARDIAN, exercises, etc. Identify and document intelligence-related findings, observations and best practices; update FP programs appropriately.

5.1.22. In coordination with AFOSI, support the development of the DTA (see paragraph 2.1.8). AFOSI may request intelligence support to ensure the DTA includes analysis of transnational/foreign terrorist TTPs, weapons (CBRNE, small arms, rocket propelled grenades [RPGs], MANPADS, improvised explosive devices [IEDs]), capabilities, activities, history, intent and probable COAs.

5.1.23. Periodically publish and disseminate an accession list to FP customers incorporating all new incoming intelligence reference materials (e.g. websites/ products).

5.1.24. Provide intelligence support and related activities (mission briefing, targeting, mission planning, GI&S support, FP threat updates, etc.) to transient units, as required.

5.1.25. IAW HHQ and MAJCOM guidance, assess and report each year on unit intelligence FP program (see paragraph 4.1.22).

5.1.26. Actively solicit FP customers' feedback to improve intelligence support processes, products and services.

## **5.2. Collection and Requirements Management.**

5.2.1. In coordination with the TWG, assist commanders in writing installation FP PIRs. In coordination with FP customers, continually assess how well FP PIRs are being satisfied to help guide intelligence and CI collection efforts. Monitor and evaluate reporting against FP requirements.

5.2.2. Manage PR program IAW HHQ and MAJCOM guidance, as appropriate. Exhaust internal, theater and national automated resources to accomplish intelligence FP support functions before forwarding requirements to outside agencies. Validate unit CRs and PRs and forward through appropriate channels.

## **5.3. Training Support**

5.3.1. Solicit and consolidate formal/special FP training requirements for all assigned and attached intelligence personnel.

5.3.2. IAW AFI 14-105 and MAJCOM guidance, establish the installation external intelligence training program tailored to the unit's mission, projected wartime tasking and base/deployment location(s).

5.3.2.1. Coordinate with AFOSI and FP customers to identify training requirements and develop an appropriate external FP threat awareness program. External training programs should address: 1) Threat Knowledge (as it applies to air base defense) 2) Visual Recognition 3) Evasion and Recovery (E&R) and 4) Collection and Reporting. Examples of external training topics include:

5.3.2.1.1. Terrorist TTPs, capabilities, activities, intentions.

5.3.2.1.2. Current threat, terrorism threat levels, advisories, alerts, warnings.

5.3.2.1.3. Nuclear Security Threat Capabilities Assessment (as appropriate) and Worldwide Asymmetric Threat to Air Force Installations, Personnel and Resources.

5.3.2.1.4. MANPADS, RPGs, IEDs, CBRNE, rockets/mortars, small arms.

5.3.2.1.5. FP legal considerations (Intelligence Oversight).

5.3.2.1.6. Locating FP threat data sources.

5.3.2.1.7. Post-mission debriefing requirements and procedures.

5.3.2.1.8. Intelligence Support to FP capabilities and limitations.

5.3.2.2. Document how the external training program will be conducted.

5.3.2.3. Provide a written evaluation of the external intelligence training program to the Operations Group Commander, Security Forces Commander and/or AFOSI Det. Commander (or equivalent) at the end of each training cycle.

5.3.3. Establish an internal FP intelligence-training program. IAW MAJCOM guidance, establish minimum qualifications for intelligence personnel to receive certification as external intelligence trainers. Ensure they are certified in areas on which they provide instruction prior to conducting training. Actively solicit customer feedback to ensure trainers meet program requirements.

5.3.3.1. All intelligence personnel should receive FP training during MQT and CT. Ensure all intelligence professionals performing FP duties receive additional training (e.g., AT Level II, Foreign Disclosure, Security Control Markings, etc.) as required. MAJCOMs can levy training requirements to satisfy unique or specialized mission areas. Ensure program qualifies intelligence personnel to perform their readiness and employment duties. All intelligence personnel will participate in the intelligence internal training program. Ensure personnel unable to attend scheduled program events receive and document make-up training on missed subjects.

5.3.3.2. Individual training records shall be updated to reflect intelligence FP training IAW HHQ and MAJCOM policy.

5.3.3.3. Internal FP training programs should address the following:

5.3.3.3.1. Terrorist groups and TTPs.

5.3.3.3.2. FP focused predictive analysis (e.g., IPB).

5.3.3.3.3. Terrorism threat methodologies, threat levels/warnings.

5.3.3.3.4. Developing tailored threat assessments.

5.3.3.3.5. TWG, FPWG and BDOC roles/responsibilities.

5.3.3.3.6. Support to FP planning, programming and operations.

5.3.3.3.7. Support to VAs, ORIs, UCIs, NSIs, and exercises.

5.3.3.3.8. Supporting development of the installation DTA.

5.3.3.3.9. Developing FP target folders.

- 5.3.3.3.10. Identifying and using FP threat data sources.
- 5.3.3.3.11. FP legal considerations (Intelligence Oversight).
- 5.3.3.3.12. Familiarization with FP policy documents.
- 5.3.3.3.13. FP customer requirements.
- 5.3.3.3.14. FP PIRs.
- 5.3.3.3.15. AFOSI roles/responsibilities.
- 5.3.3.3.16. LOAC.
- 5.3.3.3.17. E&R.

**6. Expeditionary Intelligence Responsibilities:** Responsibilities within this section should be tailored to meet the needs of the deployed location based upon the mission, environment (permissive/hostile), threats, location, etc. Duties listed below are the responsibility of the wing/installation Senior Intelligence Officer (SIO). Coordinate terrorism-related products and services with AFOSI to de-conflict responsibilities and ensure customer requirements are satisfied.

#### 6.1. Pre-deployment

- 6.1.1. Monitor unit tasking and OPLANs/Contingency Plans (CONPLANs) and advise intelligence personnel of significant changes and their impact.
- 6.1.2. Ensure adequate mobility, reception planning and preparedness for intelligence activities and personnel.
- 6.1.3. Identify intelligence personnel and equipment to support tasked FP UTCs. Act as the focal point for intelligence Air Force Specialty Code (AFSC) requirements in tasked UTCs and any deployment orders.
- 6.1.4. Monitor Air and Space Expeditionary Task Force schedule to ensure ability to fulfill commitments and manage personnel resources. Ensure personnel postured against the FP Intelligence UTCs are fully trained and qualified to fill mobility slots.
- 6.1.5. Ensure current written checklists or procedures are available for required support to mobility, reception, intelligence systems, communications architecture, Temporary Sensitive Compartmented Information Facility (T-SCIF) requirements and intelligence tasking(s). Coordinate SCI requirements with the SSO.
- 6.1.6. Submit pre-deployment FP intelligence requirements to servicing MAJCOM and coordinate necessary requirements with the appropriate theater and deployed SIOs.
- 6.1.7. Ensure intelligence GI&S requirements are identified and sufficient stocks are maintained for training and readiness, deployment and employment. Units must refer to theater guidance for additional GI&S requirements prior to deployment.
- 6.1.8. Ensure intelligence personnel provide briefing support IAW HHQ and MAJCOM directives. Briefings must incorporate the latest intelligence information tailored to the audience including appropriate FP information.
- 6.1.9. IAW 31-301, *Air Base Defense*, support security forces to ensure tasked UTCs maintain current deployment folders for locations under assigned Operational Plan

(OPLAN) taskings. Deployment folders should include country data, maps, and threat estimate.

6.1.10. Ensure FP E&R responsibilities are fulfilled IAW theater and MAJCOM guidance (e.g., Isolated Personnel Report [ISOPREP], Evasion Plan of Action [EPAs], E&R materials).

## **6.2. Collection and Requirements Management**

6.2.1. In coordination with TWG/BDOC, assist commanders in developing installation FP PIRs. In coordination with FP customers, continually assess how well FP PIRs are being satisfied to help guide intelligence and CI collection efforts. Monitor and evaluate reporting against FP requirements.

6.2.2. Manage PR program IAW MAJCOM and theater guidance, as appropriate. Exhaust internal, theater and national automated resources to accomplish intelligence support functions before forwarding requirements to outside agencies. Validate unit CRs and PRs and forward to appropriate validation authority.

6.2.3. Develop a Collection Plan, task organic ISR assets and coordinate with theater intelligence collection managers to employ ISR assets and capabilities, where applicable. Ensure de-confliction with AFOSI.

## **6.3. Employment**

6.3.1. Develop, implement and execute an FP support program as an integral part of the Wing/Base Installation/Defense Force Commander's (DFC) FP Program.

6.3.2. Allocate, assign and manage all intelligence FP personnel resources. In a deployed environment, the deployed SIO will utilize the FP Intelligence UTCs (if possible) to provide qualified intelligence personnel to meet FP requirements. Intelligence personnel supporting FP operations and missions may be operationally controlled by the supported commander and administratively controlled by the installation/wing SIO.

6.3.3. Determine appropriate intelligence requirements/tasks with FP customers and coordinate support with AFOSI. Typical requirements include: identify enemy COAs and impact of asymmetric threats on air operations based on IPB and trends/event/link analysis; conduct MANPADS threats indirect fire (IDF)/direct fire assessments; provide CBRNE IEDs, ambush and kidnapping information; provide intelligence assessments; support construction of targeting packages/target study, route analysis, media/document exploitation; Essential Element of Information (EEI) and PR management; maintain and operate intelligence databases, systems and SSO programs; identify unit support requirements and provide threat training.

6.3.4. Conduct pre-mission briefings to support Guardmount, ground patrols, convoy operations and weapons storage area missions.

6.3.5. Intelligence personnel will debrief FP operations IAW MAJCOM/theater directives. Ensure critical debrief information is disseminated rapidly to appropriate organizations (e.g. AFOSI, ATO). Follow all voice reports with written documentation. Ensure collected information is reintroduced into the intelligence cycle IAW HHQ/theater directives (e.g., Mission Report [MISREP], Intelligence Report [INTREP],

Spot Report [SPOTREP], Intelligence Summaries [INTSUM], Situation Reports [SITREP]). Develop procedures to ensure ground teams report perishable, critical information of intelligence value, including FP information.

6.3.6. Develop quality control procedures to ensure standardization and accuracy of situation/OB displays for FP considerations.

6.3.7. Ensure all organization intelligence FP functions are equipped with the required GI&S, imagery and target material products to support briefings, mission planning, staff support and employment operations.

6.3.8. Ensure pre-planned missions are updated to reflect the latest available intelligence information affecting the mission, including FP updates, and are planned to minimize the threat and enhance survivability.

6.3.9. Ensure quality control of intelligence FP mission/target folder data.

6.3.10. Ensure FP intelligence personnel assigned to mission planning functions understand their responsibilities concerning LOAC.

6.3.11. Coordinate with FP customers to identify training requirements and develop an appropriate external FP threat awareness program (see paragraph 5.3.2.1).

6.3.12. Participate in the TWG and other venues (e.g. FPWG, BDOC).

6.3.13. Analyze all-source intelligence for impact on unit mission and rapidly disseminate threat to FP customers, subordinate and lateral units, HHQs and other appropriate agencies, in coordination with AFOSI.

6.3.14. Incorporate threat information into FP planning and operations.

6.3.15. Establish procedures to track IC terrorism threat levels, terrorism warnings, alerts and advisories in coordination with AFOSI.

6.3.16. Ensure current FP checklists or procedures are available for employment operations to include as a minimum:

6.3.16.1. Intelligence support to mission planning.

6.3.16.2. OB Displays.

6.3.16.3. Briefing procedures.

6.3.16.4. Debriefing procedures.

6.3.16.5. Reporting.

6.3.16.6. Automated Intelligence Systems.

6.3.16.7. Operational Security (OPSEC) requirements and procedures.

6.3.16.8. Threat Awareness training.

6.3.17. Ensure continuity books are maintained. Continuity books should include:

6.3.17.1. AFI 14-119, AFI 10-245, AFPAM 14-118, AFTTP 3-10.1.

6.3.17.2. Theater/COCOM/Component intelligence guidance.

- 6.3.17.3. Local Operating Instructions (if applicable).
- 6.3.17.4. Vulnerability Assessment benchmarks.
- 6.3.17.5. Local TWG charter.
- 6.3.17.6. Copies of intelligence FP products (e.g. maps, overlays, briefings).
- 6.3.17.7. Intelligence portions of the installation AT plan.
- 6.3.17.8. Installation and command threat assessments (e.g. DTA).
- 6.3.17.9. FP PIR List.
- 6.3.17.10. FP Point of Contact List.
- 6.3.17.11. Intelligence Oversight Policy.
- 6.3.17.12. LOAC.
- 6.3.18. Document FP lessons learned and update FP programs appropriately (see paragraph 4.1.22).
- 6.3.19. Support AFOSI in the development of the DTA IAW AFI 10-245, *Air Force Antiterrorism (AT) Standards* (see paragraph 2.1.8). AFOSI may request intelligence support to ensure the DTA includes analysis of transnational/foreign terrorist TTPs, weapons (including CBRNE, small arms, RPGs, MANPADS, IEDs), capabilities, activities, history, intent and probable COAs.
- 6.3.20. Support/participate in SAVs, VAs and exercises IAW theater/MAJCOM guidance. Identify and document intelligence-related findings, observations and best practices. Update FP programs appropriately.
- 6.3.21. Adhere to requirements and policies contained in AFI 16-201 for disclosing classified and controlled unclassified (i.e. FOUO, tech orders, schematics, etc.) military information to foreign nationals. All classified and controlled unclassified military information must be reviewed and approved by a properly designated disclosure authority before release. Contact MAJCOM/theater Foreign Disclosure Office for guidance.
- 6.3.22. Conduct periodic reviews (at least annually) of written guidance to ensure currency, accuracy, appropriateness and applicability.
- 6.3.23. Ensure intelligence is incorporated into installation plans.
- 6.3.24. Develop and implement an intelligence unit self-assessment program.
- 6.3.25. Actively solicit feedback from wing/installation and subordinate FP customers to improve intelligence support processes, products and services.

## **7. Tenant Unit Intelligence Responsibilities**

7.1. The host wing with BOS responsibilities provides for the installation's FP. Not all the requirements listed in this AFI apply to tenant units (e.g., tenant ANG wings, field operating units, other commands). If the host unit does not have an organic intelligence capability and the tenant unit is the only organization on the base with intelligence personnel/capability assigned, the host/tenant unit agreement must define the relationship and requirements. On installations

where multiple services or nations are co-located, the host unit with BOS/FP responsibilities should develop agreements with tenant units to define relationships.

7.1. **(AETC)** At non-AETC or non-Air Force installations where AETC intelligence units are tenants, the host command (for example, AMC, AFMC, AFSOC, ACC, AFR, ANG) or host service (US Navy, US Army) of the installation is responsible for providing intelligence support to FP for that installation.

7.2. Tenant units are responsible for the following:

7.2.1. Coordinate with the installation ATO to ensure processes/procedures are in place and documented in the installation AT plan to receive threat warnings/information.

7.2.1. **(AETC)** As a minimum, tenant AETC intelligence units should be familiar with the host base antiterrorism (AT)/FP plan and local supplement, which should detail their responsibilities, if any, to the host unit.

7.2.2. Brief tenant staff, aircrews, etc., on the installation DTA.

7.2.3. In coordination with AFOSI, provide tenant staff, aircrews and other FP customers pre-deployment terrorist-related threat information.

7.2.4. Support tenant unit SAVs, VAs, ORIs, UCIs, NSIs, exercises, etc.

7.2.5. Document tenant unit activities (e.g. continuity book).

7.2.5. **(AETC)** Create a continuity book and electronic folder and keep all memorandums, requirement statements, and one copy of the most recent local FPWG and TWG minutes in it.

7.3. **(Added-AETC)** AETC units that do not have intelligence personnel assigned will designate an additional duty intelligence officer (ADIO) to provide an intelligence focal point for FP at the installation. Specifically, the installation ATO would fill the position of ADIO.

## **8. (Added-AETC) Form Adopted.**

AF Form 847, *Recommendation for Change of Publication*

DAVID A. DEPTULA, Lt Gen, USAF  
Deputy Chief of Staff, Intelligence,  
Surveillance and Reconnaissance

**(AETC)**

CARLTON D. EVERHART II, Colonel, USAF  
Deputy Director of Intelligence & Air, Space, and  
Information Operations

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

*References*

(**Added-AETC**) AFD 10-24, *Air Force Critical Infrastructure Program (CIP)*, 28 Apr 2006

JP 3-10, *Security Operations in Theater*, 1 August 2006

DOD Directive 2000.12, *DOD Antiterrorism/Force Protection (AT/FP) Program*, 18 August 2003

DOD O-2000.12H, *DOD AT Handbook*, February 2004

DOD Instruction 2000.16, *DOD Antiterrorism Standards*, Change 2, 8 December 2006

AFDD 2-4.1, *Force Protection*, 9 November 2004

AFDD 2-5.2, *Intelligence, Surveillance and Reconnaissance Operations*, 21 April 1999

AFDD 2-10, *Homeland Operations*, 21 March 2006

AFMD 39, *Air Force Office of Special Investigations*, 9 January 2006

(**Added-AETC**) AFI 10-245/AETC Sup, *Air Force Antiterrorism (AT) Standards*, 15 May 2005 (incorporating through Change 2, 20 July 2007)

(**Added-AETC**) AFI 14-105/AETC Sup 1, *Unit Intelligence Mission and Responsibilities*, 30 May 2006

AFPD 10-2, *Readiness*, 30 October 2006

AFPD 14-1, *Intelligence, Surveillance, and Reconnaissance Planning, Resources, and Operations*, 2 April 2004

AFPD 14-3, *Control, Protection and Dissemination of Intelligence Information*, 1 May 1998

AFPD 31-3, *Air Base Defense*, 28 December 2001

AFPD 71-1, *Criminal Investigations and Counterintelligence*, 1 July 1999

AFI 10-245, *Air Force Antiterrorism (AT) Standards*, 21 June 2002

AFI 14-104, *Oversight of Intelligence Activities*, 14 April 2005

AFI 14-105, *Unit Intelligence Mission and Responsibilities*, 3 June 2002

AFI 14-205, *Geospatial Information and Services*, 4 May 2004

AFI 16-201, *Air Force Foreign Disclosure and Technical Transfer Program*, 1 December 2004

AFI 25-201, *Logistic Staff*, 1 May 2005

AFI 31-201, *Security Police Standards and Procedures*, 4 December 2001

AFI 31-301, *Air Base Defense*, 15 May 2002

AFI 32-3001, *Explosive Ordnance Disposal Program*, 8 October 2004

AFI 36-2201, *Air Force Training Program*, 4 February 2005

AFI 71-101 Vol. 4, *Counterintelligence*, 1 August 2002

AFH 31-305, *Security Forces Deployment Planning Handbook*, 26 February 2003

AFMAN 37-123, *Management of Records*, 31 August 1994

AFPAM 14-118, *Aerospace Intelligence Preparation of the Battlespace*, 5 June 2001

AFTTP 3-10.1, *Integrated Base Defense*, 20 August 2004

AF Forces Command and Control Enabling Concept

Air Force Records Information Management System, (AFRIMS)

### ***Abbreviations and Acronyms***

**ABO**— Air Base Opening

**(Added-AETC) ADIO**—additional duty intelligence officer

**AFDD**— Air Force Doctrine Document

**AFH**— Air Force Handbook

**AFI**— Air Force Instruction

**AFMAN**— Air Force Manual

**AFMD**— Air Force Mission Directive

**AFFOR**— Air Force Forces

**AFOSI**— Air Force Office of Special Investigations

**AFPAM**— Air Force Pamphlet

**AFPD**— Air Force Policy Directive

**AFRC**— Air Force Reserve Command

**AFRIMS**— Air Force Records Information Management System

**AFSC**— Air Force Specialty Code

**AFTTP**— Air Force Tactics, Techniques, and Procedures

**AMC**— Air Mobility Command

**ANG**—Air National Guard

**(Added-AETC) AOR**—area of responsibility

**AT**— Antiterrorism

**ATO**— Antiterrorism Officer

**BDOC**— Base Defense Operations Center

**BOS**— Base Operating Support

**C2**— Command and Control

**CBRNE**— Chemical, biological, radiological, nuclear, high-yield explosives

**CE**— Civil Engineers  
**CENTAF**— US Central Command Air Forces  
**CI**— Counterintelligence  
**(Added-AETC) CIP**—critical infrastructure program  
**COA**— Course of Action  
**COCOM**— Combatant Command (command authority)  
**CONPLAN**— Contingency Plan  
**CONUS**— Continental United States  
**CR**— Collection Requirement  
**CRG**— Contingency Response Group  
**CSAF**— Chief of Staff of the Air Force  
**CT**— Continuation Training  
**DET**— Detachment  
**DFC**— Defense Force Commander  
**(Added-AETC) DIB**—defense industrial base  
**DNI**— Director of National Intelligence  
**DOD**— Department of Defense  
**DODD**— Department of Defense Directive  
**DODI**— Department of Defense Instruction  
**DTA**— Defense Threat Assessment  
**E & R**— Evasion & Recovery  
**EI**— Essential Element of Information  
**EOD**— Explosive Ordnance Disposal  
**EPA**— Evasion Plan of Action  
**FIR**— Field Investigation Region  
**FISS**— Foreign Intelligence and Security Services  
**FOUO**— For Official Use Only  
**FP**— Force Protection  
**(Added-AETC) FPCON**—force protection condition  
**FPI**— Force Protection Intelligence  
**FPWG**— Force Protection Working Group  
**G**— Gamma

**GI&S**— Geospatial Information and Services  
(**Added-AETC**) **GIG**—global information grid  
**GSU**— Geographically Separated Units  
**HAF**— Headquarters Air Force  
**HCS**— HUMINT Control System  
**HHQ**— Higher Headquarters  
**HUMINT**— Human Intelligence  
**IAW**— In Accordance With  
**IC**— Intelligence Community  
**IDF**— Indirect Fire  
**IED**— Improvised Explosive Device  
**IMA**— Individual Mobilization Augmentee  
**INTREP**— Intelligence Report  
**INTSUM**— Intelligence Summary  
**IPB**— Intelligence Preparation of the Battlespace  
**IQT**— Initial Qualification Training  
**ISOPREP**— Isolated Personnel Report  
**ITV**— In-Transit Visibility  
**ISR**— Intelligence, Surveillance and Reconnaissance  
**JP**— Joint Publication  
**LE**— Law Enforcement  
**LES**— Law Enforcement Sensitive  
**LOAC**— Law of Armed Conflict  
**MAJCOM**— Major Command  
**MANPADS**— Man-Portable Air Defense System  
**MISREP**— Mission Report  
**MQT**— Mission Qualification Training  
**NCO**— Non-Commissioned Officer  
**NSI**— Nuclear Surety Inspection  
**NAF**— Numbered Air Force  
**OB**— Order of Battle  
**OCONUS**— Outside Continental United States

(Added-AETC) **OPCON**—operational control  
**OPLAN**— Operations Plan  
**OPSEC**— Operational Security  
**ORI**— Operational Readiness Inspection  
**OSS/OSF**— Operations Support Squadron/Flight  
**PIR**— Priority Intelligence Requirement  
**PR**— Production Requirement  
**RDS**— Records Disposition Schedule  
**RPG**— Rocket Propelled Grenade  
**RTC**— Regional Training Center  
**SAV**— Staff Assistance Visit  
**SecAF**— Secretary of the Air Force  
**SCI**— Sensitive Compartmented Information  
**SF**— Security Forces  
(Added-AETC) **SFS**—security forces squadron  
**SME**— Subject Matter Expert  
**SIO**— Senior Intelligence Officer  
**SITREP**— Situation Report  
**SPOTREP**— Spot Report  
**SSO**— Special Security Office  
**TS**— Top Secret  
**T-SCIF**— Temporary Sensitive Compartmented Information Facility  
**TTP**— Tactics, Techniques and Procedures  
**TWG**— Threat Working Group  
**UCI**— Unit Compliance Inspection  
**UMD**— Unit Manning Document  
**USTRANSCOM**— United States Transportation Command  
**UTC**— Unit Type Code  
**VA**— Vulnerability Assessment  
**WFHQ**— Warfighting Headquarters  
**WMD**— Weapons of Mass Destruction

### *Terms*

**Administrative Control**— Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. Also called **ADCON**. (JP 0-2)

**Air Base Defense**—The local military measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks on, or sabotage of, a base to ensure that the maximum capacity of its facilities is available to US forces.

**Antiterrorism Officer**— The installation, base, regional, facility, or deploying AT advisor charged with managing the AT Program. He/she shall be a graduate of an approved Level II Course and be identified in writing by the installation and/or force commander. Reference AFI 10-245, *Air Force AT Standards*.

**Base Defense Operations Center**—A command and control facility established by the base commander to serve as the focal point for base security and defense. It plans, directs, integrates, coordinates, and controls all base defense efforts and coordinates and integrates into area security operations with the rear area operations center/rear tactical operations center. Reference AFI 31-301, *Air Base Defense*.

**Battlespace**—The commander's conceptual view of the area and factors which he/she must understand to successfully apply combat power, protect the force, and complete the mission. It encompasses all applicable aspects of air, sea, space, and land operations that the commander must consider in planning and executing military operations. The battlespace dimensions can change over time as the mission expands or contracts according to operational objectives and force composition. Battlespace provides the commander a mental forum for analyzing and selecting courses of action for employing military forces in relationship to time, tempo, and depth.

**Contingency Response Group**— An Air Force capability with effects that span the joint force, the CRG serves as the first of five force modules to assess and open air bases to extend the reach of air and space forces. They provide combatant commanders with initial Airbase Opening (ABO) and air mobility support capability during wartime, contingency, or other USTRANSCOM/AMC directed missions. CRG extend air mobility operations worldwide by deploying task organized mobility teams capable of airbase assessment, initial C2, cargo and passenger handling, in-transit visibility (ITV), quick-turn aircraft maintenance, self protection security, air traffic control, and airfield operations.

**Counterintelligence**—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. In this AFI, CI specifically refers to information about threats to Air Force installations gathered through activities conducted by the AFOSI or other service and national CI organizations.

**(Added-AETC) Critical Infrastructure Program (CIP)**—The identification, assessment, and security enhancement of cyber and physical assets and associated infrastructures essential to the execution of the National Military Strategy. It is a complementary program linking the mission

assurance aspects of the Anti-Terrorism, Force Protection, Information Assurance, Continuity of Operations, and Readiness programs (Ref. AFPD 10-24).

**Defense Force Commander**— The Defense Force Commander (DFC) is generally the senior security forces officer on station and must understand the capabilities of the base defense forces and ensure coordination with other functions and forces, on and off the installation. The DFC exercises command and control through an established chain of command. All aspects of Air Base Defense operations are directed through flight leaders and the BDOC staff. The DFC is responsible to the installation commander. Reference AFI 31-301, *Air Base Defense*.

**Defense Threat Assessment**—An all-source assessment of threats to an installation. AFOSI is responsible for the DTA. Reference DOD msg, *Standardized DOD Threat Assessment*, 22 Dec 03; AFOSI Manual 71-144 volume 7, *CI Collections, Analysis and Production*.

**Essential Elements of Information**—The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision.

**Force Protection Program**— Commander's program designed to protect Service members, civilian employees, family members, facilities, information and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services and supported by intelligence, counterintelligence and other security programs.

**Force Protection Intelligence**— Analyzed, all-source information concerning threats to DOD missions, people or resources arising from terrorists, criminal entities, foreign intelligence and security services and opposing military forces. FPI supports FP decisions and operations.

**Force Protection Working Group**— The commander's cross-functional working group made up of wing and tenant units. Working group members are responsible for coordinating and providing deliberate planning for all antiterrorism/force protection issues. The FPWG includes representatives from areas across the installation, including civil engineering, intelligence, AFOSI, security forces, public health, bioenvironmental, disaster preparedness, plans, communications, etc.

**Foreign Disclosure**—Oral or visual transmission of information through approved channels to authorized representative of a foreign government.

**Information**— Facts, data, or instructions in any medium or form.

**Integrated Base Defense**—The integrated application of offensive and defensive action, both active and passive, taken across the ground dimension of the force protection battlespace to achieve local and area dominance in support of force protection.

**Intelligence**— 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

**Intelligence Oversight**— Program developed to ensure that government entities conducting intelligence activities do not infringe on or violate the rights of US persons and operate within assigned legal parameters. Reference AFI 14-104, *Oversight of Intelligence Activities*.

**Intelligence Preparation of the Battlespace**—A systematic, continuous process of analyzing the threat and environment in a specific geographic area. It is designed to support staff estimates and military decision-making. Reference AFPAM 14-118, *Aerospace Intelligence Preparation of the Battlespace*.

**Law Enforcement Information**—Information provided by any agency chartered and empowered to enforce laws in the US; a state or political subdivision of the US; a territory, possession or political subdivision of the US; or within the borders of a host nation. Law Enforcement Sensitive (LES) information specifically refers to unclassified FOUO information that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence and the integrity of pretrial investigative reports.

**Operational Control**—Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training.

**PHOENIX RAVEN**—The PHOENIX RAVEN Program is designed to ensure adequate protection for aircraft transiting airfields where security is unknown or deemed inadequate to counter local threats. Teams of two to four specially trained and equipped Security Forces personnel deploy to deter, detect, and counter threats to personnel/aircraft by performing a variety of duties (e.g. close-in aircraft security, advising aircrews on FP measures, accomplishing airfield assessments to document existing security measures and vulnerabilities).

**Priority Intelligence Requirement**—Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision-making.

**Terrorism**—The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

**Terrorism Threat Level**—An intelligence threat assessment of the level of terrorist threat faced by US personnel and interests in a foreign country. The assessment is based on a continuous intelligence analysis of a minimum of four elements: operational capability, intentions, activity and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT and HIGH. Threat levels should not be confused with force protection conditions. Threat level assessments are provided to senior leaders to assist them in determining the appropriate local force protection condition. (Department of State and Department of Homeland Security also make threat assessments, which may differ from those determined by Department of Defense.)

**Threat Working Group**— The commander’s Force Protection advisory body for tactical and immediate recommendations on mitigating or countering threats for an installation. A TWG is composed of personnel from several functional areas, most commonly: Intelligence, Security Forces, AFOSI, AT Officer, Medical, Communications, Civil Engineering and Operations. It is not a FPWG; TWG’s provide the threat information to the FPWG. Further guidance for the TWG is found in AFI 10-245, *Air Force AT Standards*.

**Unit**—A unit is defined as squadron level and/or above.

**US Persons**— The term “United States Person” applies to the following:

- (1) A United States citizen.
- (2) An alien known by the DOD intelligence component concerned to be a permanent resident alien. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.
- (3) An unincorporated association substantially composed mostly of United States citizens or permanent resident aliens.
- (4) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

**Vulnerability Assessment**— A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism.

**Warfighting Headquarters**—The Air Force Forces Command and Control Enabling Concept states the Air Force must provide air, space and information operations capabilities to unified combatant commanders in support of their strategic objectives across the full range of military operations. The Air Force must be able to not only provide the forces, ready and able to deploy quickly and employ globally, but also to provide the command, control and support of those forces and operations. Operational level C2 must focus on effects-based results, across the full range of military operations, to achieve our nation’s military objectives. The WFHQ is the component-level organization through which the AF will provide these capabilities.

## Attachment 2 (Added-AETC)

## CIP INTELLIGENCE REQUIREMENTS

**A2.1. (Added-AETC) Requirements.** Figure A2.1 (Added) lists the CIP intelligence requirements recommended for incorporation by host units in their intelligence collection plans. Essential elements of information are the commander's most critical information requirements regarding the adversary and the environment. They provide amplification for the intelligence community on the type of information needed to evaluate the overall threat for each of the CIP intelligence requirements.

**Figure A2.1. (Added) CIP Intelligence Requirements.**

<b>Sources of Threats</b>	
	Hostile states (military, paramilitary, intelligence and security)
	Criminals (including terrorists)
	Insiders
<b>Types of Threats</b>	
	Kinetic (conventional, weapons of mass destruction)
	Cyber
	Other nonkinetic
<b>Information Collection and Surveillance of Critical Infrastructure (Figure A2.2 (Added))</b>	
(1a)	Surveillance of Department of Defense (DoD) critical infrastructure
(1b)	Surveillance of civil critical infrastructure
(1c)	Collection of information about personnel strength or readiness status
(1d)	Collection of information about DoD capabilities, operations, or dependencies
<b>Preparatory Activities for Attacks on Critical Infrastructure (Figure A2.3 (Added))</b>	
(2a)	Proximity of potential adversaries to critical infrastructure
(2b)	Indications of impending hostile activity against physical infrastructure
(2c)	Cyber activity in preparation for hostile action
<b>Specific and General Threats of Attacks on Critical Infrastructure (Figure A2.4 (Added))</b>	
(3a)	Threats to DoD critical infrastructure
(3b)	Threats to civil critical infrastructure
(3c)	Threats to DoD personnel
(3d)	Cyber threats or challenges to critical infrastructure
<b>Origin and Nature of Attacks Against Critical Infrastructure (post-event) (Figure A2.5 (Added))</b>	

**Figure A2.2. (Added) Information Collection and Surveillance of Critical Infrastructure.**

<b>(1a) Surveillance of DoD critical infrastructure</b>	
1	Attempts to discover locations of:
1.1	DoD financial service sites
1.2	Intelligence, surveillance, and reconnaissance (ISR) sector sites, ground controlling stations and facilities
1.3	DoD logistics and supply sites
1.4	Ammunition facilities
1.4.1	Ammunition depots
1.4.2	Ammunition production facilities

1.5	Petroleum facilities
1.5.1	Petroleum transport (pipelines)
1.5.2	Petroleum bulk storage
1.6	Ports, harbors, and airfields
1.7	DoD transportation sites (including command sites, air mobilization terminals, air traffic control systems, etc.)
1.8	Global information grid (GIG) sites or systems
1.8.1	Network router sites
1.8.2	Defense Enterprise Computing Centers
1.8.3	Telecom hotels
1.9	DoD hospitals and medical centers
1.10	Embassies
2	Solicitation and collection of information about:
2.1	DoD financial service sites
2.2	ISR sector sites, ground controlling stations and facilities
2.3	DoD logistics and supply sites
2.4	Ammunition facilities
2.5	Petroleum facilities
2.6	Ports, harbors, and airfields
2.7	DoD transportation sites (including command sites, air mobilization terminals, air traffic control systems, etc.)
2.8	GIG sites or systems
2.9	DoD hospitals and medical centers
2.10	Embassies
3	Suspicious contacts or events:
3.1	Proximity to:
3.1.1	DoD financial service sites
3.1.2	ISR sector sites, ground controlling stations and facilities
3.1.3	DoD logistics and supply sites
3.1.4	Ammunition facilities
3.1.5	Petroleum facilities
3.1.6	Ports, harbors, and airfields
3.1.7	DoD transportation sites (including command sites, air mobilization terminals, air traffic control systems, etc.)
3.1.8	GIG sites or systems
3.1.9	DoD hospitals and medical centers
3.1.10	Embassies
3.2	Originator of report
3.2.1	Personnel affected
3.2.2	Law enforcement official
3.2.3	Other official observer
3.2.4	Unofficial observer
3.2.5	Commercial establishment
3.3	Suspicious inquiries about:
3.3.1	Military members

3.3.2	Dependents
3.3.3	Other related personnel
3.4	Suspect activities
3.4.1	Unusual photography
3.4.2	Shadowing
3.4.3	Unauthorized access to housing areas
<b>(1b) Surveillance of civil critical infrastructure</b>	
1	Attempts to discover locations of:
1.1	Transportation infrastructure (rail system, highways, bridges, tunnels, airports, seaports)
1.2	Power plants
1.3	Commercial public works sites
1.4	Dams and waterways
1.5	Defense industrial base (DIB) facilities, industrial sites, workers, and supporting infrastructure
2	Solicitation and collection of information about:
2.1	Transportation infrastructure (rail system, highways, bridges, tunnels, airports, seaports)
2.2	Power plants
2.3	Commercial public works sites
2.4	Dams and waterways
2.5	DIB facilities, industrial sites, workers, and supporting infrastructure
3	Suspicious contacts or events
3.1	Proximity to:
3.1.1	Transportation infrastructure (rail system, highways, bridges, tunnels, airports, seaports)
3.1.2	Power plants
3.1.3	Commercial public works sites
3.1.4	Dams and waterways
3.1.5	DIB facilities, industrial sites, workers, and supporting infrastructure
3.2	Originator of report
3.2.1	Personnel affected
3.2.2	Law enforcement official
3.2.3	Other official observer
3.2.4	Unofficial observer
3.2.5	Commercial establishment
3.3	Suspicious activity report about:
3.3.1	Inquiries of
3.3.2	Facility workers
3.3.3	Dependents of facility workers
3.3.4	Other related personnel
3.4	Suspect activities
3.4.1	Unusual photography
3.4.2	Shadowing
3.4.3	Unauthorized access to housing areas
<b>(1c) Collection of information about personnel strength or readiness status</b>	
1	Inquiries of:
1.1	Military members

1.2	Dependents
1.3	Other related personnel
2	Suspect activities
2.1	Unusual photography
2.2	Shadowing
2.3	Unauthorized access to housing areas
2.4	Unauthorized access to DoD commissaries, schools, recreation facilities
2.5	Impersonation
3	Cyber activity
3.1	Unauthorized access to military personnel systems
3.2	Inquiries about defense information or control networks
3.3	Probing of defense networks
<b>(1d) Collection of information about DoD capabilities, operations, or dependencies</b>	
1	Inquiries about:
1.1	ISR systems and capabilities
1.2	Space systems and capabilities
1.3	Logistics systems and capabilities
1.4	Dependencies on commercial public works infrastructure
1.5	Deployment schedules and troop movements
1.6	Dependencies on commercial transportation infrastructure
1.7	DoD GIG dependencies on commercial telecommunication infrastructure
1.8	DoD health affairs systems, capabilities and dependencies on public health infrastructure
1.9	Advanced technologies
2	Extensive electronic information gathering
2.1	Extensive Web searches for DoD information
2.2	Attempted data mining for DoD information

**Figure A2.3. (Added) Preparatory Activities for Attacks on Critical Infrastructure.**

<b>(2a) Proximity of potential adversaries to critical infrastructure</b>	
1	Movements into proximity
1.1	Criminal movements
1.2	Terrorist movements
1.2.1	Into proximity
1.2.2	Departure of subject matter expert
1.3	Military paramilitary movements
1.3.1	Overt
1.3.2	Covert
2	Identification in proximity
2.1	Criminals
2.2	Terrorists
2.2.1	Local nationals
2.2.2	Foreigners
2.2.3	Known suspected subject matter expert
2.2.4	Discovery of criminal and terrorist infrastructure (such as, safe house)

2.3	Military and paramilitary
<b>(2b) Indications of impending hostile activity against physical infrastructure</b>	
1	Indications of:
1.1	Target selection
1.2	Reconnaissance and final surveillance of targets
1.3	Commitment or transfer of funding for attack
1.4	Rehearsal of attack
1.5	Communications to proceed with attack
<b>(2c) Cyber activity in preparation for hostile action</b>	
1	Increased unauthorized cyber activity
1.1	Chatter
1.2	Probing
1.3	Incidents (such as, Web site defacing)
2	Heightened malicious code activity
3	Inquiries about defense information or control networks

**Figure A2.4. (Added) Specific and General Threats of Attacks on Critical Infrastructure.**

<b>(3a) Threats to DoD critical infrastructure</b>	
1	Originator of threat
1.1	Known or unknown
1.2	History of
1.2.1	Carrying out threats
1.2.2	Other criminal activity (including terrorism)
2	Medium of threat communication
3	Initial recipients of threat
4	Specific contents of threat
4.1	Targets
4.1.1	Region area
4.1.2	Facilities
4.1.2.1	Military bases
4.1.2.1.1	Military base in general
4.1.2.1.2	Specific base elements
4.1.2.2	ISR sector sites, ground controlling stations, and facilities
4.1.2.3	DoD financial service sites
4.1.2.4	DoD hospitals and medical centers
4.1.3	Infrastructure
4.1.3.1	Transportation
4.1.3.1.1	Ports
4.1.3.1.2	Airports
4.1.3.1.3	DoD transportation sites (including command sites, air mobilization terminals, air traffic control systems, etc.)
4.1.3.1.4	Dams and waterways
4.1.3.1.5	Railways
4.1.3.2	DoD logistics and supply sites

4.1.3.3	Ammunition facilities
4.1.3.4	Petroleum facilities
4.1.3.5	Telecommunications
4.1.3.6	Dams and waterways
4.1.4	Electrical power
4.1.4.1	Generation
4.1.4.2	Transmission
4.1.4.3	Distribution
4.2	Timing
4.3	Location
4.4	Intended effect
5	Demands
<b>(3b) Threats to civil critical infrastructure</b>	
1	Originator of threat
1.1	Known or unknown
1.2	History of
1.2.1	Carrying out threats
1.2.2	Other criminal activity (including terrorism)
2	Medium of threat communication
3	Initial recipients of threat
4	Specific contents of threat
4.1	Targets
4.1.1	Region area
4.1.2	Facilities
4.1.2.1	Defense industry facilities
4.1.2.1.1	DIB workers
4.1.2.1.2	Supporting infrastructure for DIB
4.1.3	Infrastructure
4.1.3.1	Transportation
4.1.3.1.1	Ports
4.1.3.1.2	Airports
4.1.3.1.3	Depots and transshipment points
4.1.3.1.4	Motor pools
4.1.3.2	Telecommunications
4.1.3.3	Dams and waterways
4.1.3.4	Electrical power
4.1.3.4.1	Generation
4.1.3.4.2	Transmission
4.1.3.4.3	Distribution
4.1.4	Potable water supplies
4.1.5	Food supplies
4.1.6	Health affairs infrastructure
4.1.6.1	Emergency care facilities
4.1.6.2	Blood supplies
4.1.6.3	Drug and chemical supplies

4.2	Timing
4.3	Location
4.4	Intended effect
5	Demands
<b>(3c) Threats to DoD personnel</b>	
1	Originator of threat
1.1	Known or unknown
1.2	History of
1.2.1	Carrying out threats
1.2.2	Other criminal activity (including terrorism)
2	Medium of threat communication
3	Initial recipients of threat
4	Specific contents of threat
4.1	Individual, groups of military, and government personnel
4.1.1	Named individuals
4.1.2	US citizens and other noncombatants eligible for noncombatant emergency operation in overseas locations
4.2	Military and government personnel administrative, assembly, and mobilization points
4.3	Military and family housing
4.4	Force Protection capabilities
5	Demands
<b>(3d) Cyber threats or challenges to critical infrastructure</b>	
1	Originator of threat
1.1	Known or unknown
1.2	History of
1.2.1	Carrying out threats
1.2.2	Other criminal activity (including terrorism)
2	Medium of threat communication
3	Initial recipients of threat
4	Specific contents of threat
4.1	Targets
4.1.1	Banking and financial services industries
4.1.2	Power-generating industries
4.1.3	Military telecommunications
4.1.4	Civil telecommunications
4.1.5	Infrastructure supervisory control and data acquisition systems
4.2	Timing
4.3	Location
4.4	Intended effect
5	Demands

**Figure A2.5. (Added) Origin and Nature of Attacks Against Critical Infrastructure (post-event).**

1	Attack event
---	--------------

1.1	Location of event
1.2	Type of event
1.3	Magnitude of event
1.4	Personnel killed and injured
1.5	Property and equipment damaged
2	Attack origin
2.1	Responsible group
2.1.1	Military members
2.1.2	Dependents
2.1.3	Other related personnel
2.2	Suspect activities
2.2.1	Unusual photography
2.2.2	Shadowing
2.2.3	Unauthorized access to housing areas

## Attachment 3 (Added-AETC)

## INTELLIGENCE SUPPORT CHECKLISTS

Table A3.1. (Added) In Garrison Checklist.

I T E M	A	B
	Process	Complete
1	Provide significant force protection intelligence related to AFOSI and SFS; if necessary active the FPWG, TWG, and BDOC.	
2	Participate in all FPWGs, TWGs, and BDOC meetings (real world or exercise).	
3	Participate and add intelligence value to installation vulnerability assessments during FPWGs and TWGs.	
4	Conduct internal and external intelligence training on a semi-annual basis or as needed on intelligence support to force protection issues relevant to unit operations (this includes squadron intelligence personnel) to include: <ul style="list-style-type: none"> <li>- Analytical focus on intelligence message traffic</li> <li>- Online sites or homepages containing FP data</li> <li>- Deployed intelligence support to FP responsibilities</li> </ul>	
5	Maintain a reference list of intelligence websites or documents relating to terrorist and host nation threat data for in garrison and programmed deployment bases. Include: <ul style="list-style-type: none"> <li>- Mood of local and indigenous population as reported by AFOSI</li> <li>- Known and identified terrorist groups</li> <li>- Historical incidents/targeting</li> <li>- AFOSI assessments on local criminal elements</li> <li>- Country restrictions</li> <li>- FPCON levels</li> <li>- In-place procedures</li> <li>- Any vulnerability threat assessments from AFOSI</li> </ul>	
6	Disseminate intelligence related to FP info: <ul style="list-style-type: none"> <li>- Via read files, web page, and message</li> <li>- Include FP related intelligence issues in current intelligence briefing (CIB) regularly or at least quarterly</li> </ul>	

Table A3.2. (Added) Predeployment Checklist.

I T E M	A	B
	Process	Complete
1	Once unit is identified for possible deployment, monitor AOR events if not already being done.	

<b>2</b>	If it is a short-notice deployment, contact the local AFOSI detachment. - Inform them of possible deployment location and help arrange for unit to receive counterintelligence threat information.	
<b>3</b>	Once deployment location is identified, check files and intelligence databases/sources for issues and threats. - Submit request for information and /PRs as needed to the numbered Air Force - Obtain imagery information from the 480 <sup>th</sup> Inspector General home page	
<b>4</b>	Coordinate with TWG to provide commanders with overall assessment.	
<b>5</b>	Ensure all relevant intelligence information is included in unit deployment briefing and chalk briefing.	

**Table A3.3. (Added) Employment/Sustainment Checklist.**

<b>I T E M</b>	<b>A</b>	<b>B</b>
	<b>Process (After arrival at deployment site)</b>	<b>Complete</b>
<b>1</b>	Contact onsite SFS and AFOSI. - Establish FPWG - Verify the TWG schedule - Establish intelligence support requirements (maps, charts)	
<b>2</b>	Create and maintain local read files (at appropriate classification levels).	
<b>3</b>	Ensure SIPRNET and JWICS connectivity are established.	
<b>4</b>	Coordinate with local intelligence agencies, to include: - US Embassy (AFOSI coordination) - Host nation security (AFOSI coordination) - Other US service organizations (USN, USA, USMC) - Other coalition and multinational organizations as required	
<b>5</b>	Ensure intelligence provides FP related intelligence to SFS, AFOSI, and appropriate commanders in a timely manner.	
<b>6</b>	Contact theater J2/JISE. - Coordinate all FP-related PRs through the J2/JISE or home station if necessary - Contact J2/JISE at a minimum three times a week for relevant reports and information - Work imagery requests through JTF J2/JISE - J2/JISE should continue to provide data to the FP cell	
<b>7</b>	Coordinate all intelligence support to FP requirements with the TWG and submit PRs as needed.	
<b>8</b>	Check with local AFOSI for additional information and reporting.	
<b>9</b>	Ensure deployed unit is receiving FP related intelligence and message traffic updates.	
<b>10</b>	Coordinate with local intelligence personnel to ensure:	

<b>I T E M</b>	<b>A</b>	<b>B</b>
	<b>Process</b> <b>(After arrival at deployment site)</b>	<b>Complete</b>
	<ul style="list-style-type: none"> <li>- Read files are updated</li> <li>- Message traffic includes FP-related intelligence</li> <li>- Updates on local anti-terrorism restrictions and security measures are provided</li> <li>- FP issues relating to intelligence are included in current intelligence briefing</li> <li>- The SIO is informed of all “hot” issues and back briefed on breaking issues</li> </ul>	

**Table A3.4. (Added) Redeployment Checklist.**

<b>I T E M</b>	<b>A</b>	<b>B</b>
	<b>Process</b>	<b>Complete</b>
<b>1</b>	With the FPWG, coordinate with senior leadership as to exactly when operations and coverage will cease.	
<b>2</b>	FPWG must continue receiving intelligence support until all personnel have departed deployed location: <ul style="list-style-type: none"> <li>- AFOSI is still able to obtain information from their sources</li> </ul>	

**Table A3.5. (Added) Exercise Checklist.**

<b>I T E M</b>	<b>A</b>	<b>B</b>
	<b>Process</b>	<b>Complete</b>
<b>OBJECTIVE:</b> In addition to in-garrison, predeployment, employment/sustainment, and redeployment actions, the following actions need to be accomplished for local and major exercises.		
<b>1</b>	Coordinate AT/FP threat scenarios with the TWG for realism during exercises.	
<b>2</b>	<b>FEEDBACK:</b> Document intelligence support to FP lessons learned and forward to HQ AETC/A2OI for inclusion into lessons learned databases.	